Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 23 June 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Minerals Management Service is working diligently to secure offshore oil and gas production in order to maintain continuity of oil and gas supplies in the Gulf of Mexico during the 2005 hurricane season. (See item 1)
- The Cincinnati Enquirer reports the Kentucky Office of Homeland Security staged an "agroterrorism" exercise designed to improve the communications and response of the agencies, local governments, first−responder police and fire crews and others that would respond to an agroterrorism event or attack. (See item 11)
- The New York Times reports the National Institute of Standards and Technology has recommendations that include fundamental changes in the planning, construction, and operation of skyscrapers to help people survive not only terrorist attacks but also accidental or natural calamities. (See item 28)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 21, Minerals Management Service* — **Securing offshore oil and gas production in the 2005 hurricane season.** The 2004 hurricane season brought home to the American public the importance of oil and gas resources in the Gulf of Mexico. The Minerals Management Service

(MMS) is working diligently to ensure that all systems are in place to maintain continuity of oil and gas supplies during the 2005 season, and once again emerge with no loss of life or significant pollution. This is particularly important because 2005 is anticipated to be another above average hurricane season. “MMS manages the design and approval of extensive offshore drilling structures in the Gulf of Mexico,” said Chris Oynes, Regional Director, Gulf of Mexico Region. “It is our goal to ensure the safety of workers, protect the environment from oil spills and prevent the long−term disruption of gas and oil production.” MMS manages offshore activities that generate 30 percent of America’s domestic oil and 21 percent of America’s domestic natural gas. “The key points are preparedness and safety. Through the dedicated work of MMS and the strong partnerships with the U.S. Coast Guard, other government agencies and the oil and gas industry, we will do our best to prepare for this storm season,” said Tom Readinger, Associate Director, Offshore Minerals Management.
Minerals Management Service: http://www.mms.gov/
Source: http://www.mms.gov/ooc/press/2005/press0621.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *May 20, Government Accountability Office* — **GAO−05−462: Perchlorate: A System to Track Sampling and Cleanup Results Is Needed (Report).** Perchlorate, a primary ingredient in propellant, has been used for decades in the manufacture and firing of rockets and missiles. Other uses include fireworks, flares, and explosives. Perchlorate has been found in drinking water, groundwater, surface water, and soil in the United States. The National Academy of Sciences (NAS) reviewed studies of perchlorate’s health effects and reported in January 2005 that certain levels of exposure may not adversely affect healthy adults but recommended more studies be conducted on the effects of perchlorate exposure in children and pregnant women. The Government Accountability Office (GAO) determined (1) the estimated extent of perchlorate in the United States, (2) what actions have been taken to address perchlorate, and (3) what studies of perchlorate’s health risks have reported. GAO recommends that Environmental Protection Agency (EPA) work with Federal agencies and the States to establish a structure to track and monitor perchlorate detections and cleanup efforts. EPA agreed with GAO's findings but the Department of Defense (DoD) did not. Neither agency agreed with GAO's recommendation. GAO believes its findings are sound; further, DoD’s citation of sites not on EPA’s list underscores the need for this recommendation.
Highlights: http://www.gao.gov/highlights/d05462high.pdf
Source: http://www.gao.gov/new.items/d05462.pdf

[Return to top]

Defense Industrial Base Sector

3. *June 22, Associated Press* — **Airbus picks Alabama for new plant.** The European Aeronautic Defense and Space Co. (EADS), the parent company of European aircraft maker Airbus, seeking to better compete with Boeing for a lucrative Air Force contract to build military refueling tankers, announced Wednesday, June 22, it has selected Mobile, AL, over three other

Southern sites for a $600 million factory. Ralph D. Crosby, chairman and CEO of EADS North America, said Mobile was chosen because it is "strategically located" on the Gulf of Mexico, and offers a skilled work force, airport runways and a deep−water port. Brookley Industrial Complex provides 4.5 million square feet of industrial space, and includes access to the Mobile downtown airport. An Airbus engineering center will be built nearby and is expected to open in 2006, the company said. The Boeing Co., based in Chicago, lost the tanker deal last year after revelations that it had hired a top Air Force acquisitions official who later admitted giving the company preferential treatment. Initially, EADS plans an engineering center that would employ 100 to 150 people. If the company wins the tanker contract, it would then team with a U.S. defense contractor to build the factory, which could employ as many as 1,100 people.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/22/AR2005062200857.html

[Return to top]

Banking and Finance Sector

4. *June 22, Washington Post* — **Ubiquitous technology, bad practices drive up data theft.** Collectively, nearly 50 million accounts have been exposed to the possibility of identity fraud since the beginning of the year, a significant increase from last year. Security experts, law enforcement officials and privacy advocates agree that while computer crime is on the rise, it is hardly new. The escalations are because, in part, organizations are telling their customers or employees about incidents more than they used to. However, experts see other factors contributing to the data−theft siege. A boom in data collection has created a marketplace of valuable information stored on computers in thousands of places, many with weak security. "The current fiascos in cyber−security have been occurring for the past 10 years," said Tom Kellermann, who recently left his position as senior data risk management specialist for the World Bank. Kellermann and others blame poorly designed software, inattention to data security and an under appreciation of the problem by top management in corporations and other institutions. Simultaneously, some hackers who used to get their kicks merely being disruptive are pooling efforts with organized criminals, said Jonathan J. Rusch, a special counsel in the fraud section of the Department of Justice.
Security Breaches in 2005: http://www.washingtonpost.com/wp−dyn/content/graphic/2005/06/22/GR2005062200071.html
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/21/AR2005062101615.html

5. *June 22, InformationWeek* — **Banks scramble to contain damage from CardSystems hacking incident.** Banks that issue credit and debit cards are moving rapidly to contain the damage caused by the potentially massive theft of card information from a transaction−processing company that was disclosed last week. Some 22 million Visa−branded cards and 14 million MasterCard−branded cards were exposed to the security breach at CardSystems Solutions Inc. that was disclosed by MasterCard last week. The breach was reported by CardSystems to Visa and MasterCard in late May. Washington Mutual has canceled 1,400 cards whose numbers were stolen and is issuing replacements. J.P. Morgan Chase & Co., which with 94 million cards outstanding is the nation's largest card issuer, hasn't canceled or reissued any cards as a result of the incident but is monitoring the situation closely,

a spokesperson says. Visa and MasterCard are relaying information picked up by their fraud−detection systems to issuing banks, which then decide whether to cancel or reissue cards. The 1,400 cards canceled by Washington Mutual are known to have been used to commit fraud; an unknown but presumably higher number may be at risk for fraud, a bank spokesperson said.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=JFVBM1XPRJFR4QSNDBGCKH0CJUMEKJVN?articleID=164901831

6. *June 22, Evening News (Scotland)* — **Finance world's biggest security threat now comes from within.** Internal security breaches have overtaken external IT attacks as the biggest threat to the world's financial institutions as hackers switch their focus from technology to people. Deloitte's 2005 Global Security Survey of senior security officers at the top 100 financial institutions found less than a third experienced an IT security breach in the past 12 months, down from 83 percent in 2004. However, the extent of internal breaches more than doubled, with 35 percent encountering attacks from the inside, compared to only 14 percent in the previous 12 months. Director of security services at Deloitte, Mike Maddison, said: "Technological loopholes are being closed, but the hackers' tactics have now shifted towards manipulating human behavior as we've seen from the explosion in phishing attacks." "People are now the point of weakness, and financial institutions will have to change their focus in the same way that the hackers have," said Maddison.
Survey: http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005−06−22b.pdf
Source: http://business.scotsman.com/technology.cfm?id=687182005

[Return to top]

Transportation and Border Security Sector

7. *June 22, Associated Press* — **Biometrics ID system debuts at Orlando International Airport.** A private company hopes as many as 30,000 other people this year will follow the lead of the security chief at Orlando International Airport by offering up their biometric information for a program guaranteeing travelers an exclusive security line, and the promise of no random secondary pat−downs, in exchange for a background check by the Department of Homeland Security. The privately run program debuted Tuesday, June 21, at Orlando, FL's International Airport, the first and so far only airport that is trying it out. Those passengers who pay $80 a year to join the traveler pilot program called "Clear" register by computer either at home or at the airport and give their biometric data at an airport kiosk resembling an oversize ATM machine. The information is then submitted to the Transportation Security Administration. If the passengers are approved, they earn the right to go through a separate, quicker security lane as soon as July, although they still will need to pass shoeless through an airport metal detector. Similar systems exist at some European airports and in five U.S. airports as a part of a free test by the TSA, but the government program has been capped at 10,000 participants and cards at one airport don't work at others.
Source: http://www.usatoday.com/travel/flights/2005−06−21−biometric− orlando_x.htm

8. *June 22, St. Petersburg Times (FL)* — **Tampa port reluctant to impose fees for security.** The Tampa Port Authority probably won't adopt shipping fees proposed by a Florida seaports group to pay for escalating security costs. The Florida Port Conference, which includes officials from

the state's 13 deep−water ports, voted June 8 to adopt minimum security charges, including $1 per multiple−day cruise passenger, $2 per cargo container and higher docking and cargo fees. But the Tampa Port Authority abstained from voting and will look at ways to reduce security costs before considering the fees, said port director Richard Wainio. Jacksonville port officials also abstained and Key West voted no. Wainio said Tuesday, June 21, that he wants to find ways to rein in security costs before imposing new fees on shippers, who pay for security improvements through general port fees. Ports are free to adopt the consortium's recommended fees, charge higher ones or ignore them. Wainio told the port authority's board Tuesday the agency is well positioned to land state grants for maritime business projects. New growth management legislation provides some $500−million for transportation improvements across Florida, he said. Ports across the country are struggling to pay for security improvements required by the federal government since the 9/11 attacks.
Source: http://www.sptimes.com/2005/06/22/Business/Tampa_port_reluct ant_.shtml

9. *June 22, Government Accountability Office* — **GAO−05−835T: Commercial Aviation: Preliminary Observations on Legacy Airlines' Financial Condition, Bankruptcy, and Pension Issues (Testimony).** Since 2001, the U.S. airline industry has confronted unprecedented financial losses. Two of the nation's largest airlines −− United Airlines and US Airways −− went into bankruptcy, terminating their pension plans and passing the unfunded liability to the Pension Benefit Guaranty Corporation (PBGC). PBGC's unfunded liability was $9.6 billion; plan participants lost $5.2 billion in benefits. Considerable debate has ensued over airlines' use of bankruptcy protection as a means to continue operations, often for years. Many in the industry and elsewhere have maintained that airlines' use of this approach is harmful to the industry, in that it allows inefficient carriers to reduce ticket prices below those of their competitors. This debate has received even sharper focus with pension defaults. Critics argue that by not having to meet their pension obligations, airlines in bankruptcy have an advantage that may encourage other companies to take the same approach. The Government Accountability Office's testimony presents preliminary observations in three areas: (1) the continued financial difficulties faced by legacy airlines, (2) the effect of bankruptcy on the industry and competitors, and (3) the effect of airline pension under funding on employees, retirees, airlines, and the PBGC.
Highlights: http://www.gao.gov/highlights/d05835thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−835T

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

10. *June 22, Agence France Presse* — **China reports new foot−and−mouth disease outbreak.** China has reported another outbreak of foot−and−mouth disease which infected 40 head of cattle, the United Nation's Food and Agriculture Organization (FAO) told AFP. The outbreak

was discovered in Weili county, in central Xinjiang region, FAO's representative Noureddin Mona said Wednesday, June 22. To stop the spread of the disease, authorities culled 261 cows, including the 40 infected ones and those raised near them, Mona told AFP. The outbreak was revealed after the Ministry of Agriculture (MOA) last month claimed the disease was under control after four outbreaks occurred from April to May, prompting authorities to cull more than 4,000 cattle. The outbreaks occurred in the provinces of Hebei, Shandong, Jiangsu, the Xinjiang region, and Beijing, the MOA said. It was a rare acknowledgement from China that foot−and−mouth exists inside its borders. Outside observers suspect China of being the origin of several foot−and−mouth epidemics in recent years, including a 1997 outbreak in Taiwan which was the first to strike the island in 68 years.
Source: http://news.yahoo.com/s/afp/20050622/hl_afp/healthchinafarm_050622115351;_ylt=AqMyeaJc4iQ8JOTYxVM9qeuJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

11. *June 22, Cincinnati Enquirer (OH)* — **Agroterrorism exercise held in Kentucky.** The Kentucky Office of Homeland Security staged an "agroterrorism" exercise in Northern Kentucky attended by more than 200 people from about 80 agencies. Under the scenario, terrorists infiltrate a goat show and expose several animals to a bioagent, which then begins to spread. The exercise is designed to improve the communications and response of the agencies, local governments, first−responder police and fire crews and others that would respond to an agroterrorism event or attack. The daylong exercise was at Northern Kentucky University's Metropolitan Education and Training Services Center corporate training center. The exercise is to continue Wednesday, June 22, at the University of Kentucky Research Center. Those participating will don protective gear to herd animals, burn bales of hay exposed to infectious materials, and undertake other hands−on training, said Andrew Cline, deputy state director of homeland security. Veterinarian Paul Garofolo said the exercise was valuable, particularly as it related to the quick dissemination of information about potential agroterrorism threats. "You learn how the instant−management system works, and you learn in a real scenario how information can be transferred from one organization to another and how things are supposed to work in a true emergency."
Source: http://news.enquirer.com/apps/pbcs.dll/article?AID=/20050622/NEWS0103/506220388

12. *June 21, Reuters* — **Austria finds second case of mad cow disease.** A case of mad cow disease has been found in Austria, the second in the country's history, the health and agriculture ministers said on Tuesday, June 21. The ministers called a news conference to announce the case of the brain−wasting disorder, or bovine spongiform encephalopathy (BSE). The disease was found during a routine test on an 11−year−old cow from a small farm of seven cattle near the German border in the western province of Vorarlberg. All seven animals were slaughtered and cremated. Agriculture Minister Josef Proell said it was a standard safety procedure in Austria for cattle older than 24 months that die of unknown causes to be tested for BSE. As this cow died unexpectedly in late May after showing suspicious signs including tiredness, it was tested. How the animal became infected was not clear, said Josef Koefer, divisional head at Austrian food safety agency.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=topNews&storyID=2005−06−21T193459Z_01_KNE157834_RTRUKOC_0_HEALTH−BSE−AUSTRIA.xml

[Return to top]

Food Sector

13. *June 22, Agence France Presse* — **European Union food safety agency launched.** The European Food Safety Authority (EFSA), opened amid great ceremony in Parma, Italy, is charged with ensuring healthy eating for hundreds of millions of Europeans and will have a staff of hundreds and a budget of millions to help it do so. "EFSA is a young organization with progress still to make, but it has already accomplished considerable work in publishing more than 200 scientific opinions in two years," Geoffrey Podger, executive director of the authority, said. "At the moment we have 65 experts belonging to the EFSA, and this figure should rise to 100 at the end of the year, and we rely on a network of 500 external scientific experts," Hermann Koeter, EFSA's scientific director, said. The authority's job is to provide independent scientific advice to risk managers on all issues related to the safety of foodstuffs destined for human and animal nourishment, according to an authority document. Its remit covers areas as diverse as mad cow disease, genetically−modified organisms, pesticides, and food additives. It operates through eight specific working groups on any issue arising from the safety of the food chain.
Source: http://www.todayonline.com/articles/57391.asp

14. *June 22, USAgNet* — **Mad cow case still impacting jobs in U.S. meat industry.** The American Meat Institute (AMI) said that the U.S. meat−processing industry lost 7,800 jobs since May 2003 −− when Canada confirmed its first case of mad cow disease or bovine spongiform encephalopathy (BSE) and the U.S. closed its market to live Canadian cattle imports. AMI cited recently released U.S. Bureau of Labor Statistics (BLS) data. According to the BLS, in May 2003, the U.S. meat industry employed 153,100 people. However, but by April 2005, employment declined to 143,300 people. According to AMI president J. Patrick Boyle, many U.S. beef slaughter plants −− especially those on the U.S.−Canadian border −− were built on the border because they could rely upon a steady supply of Canadian cattle. But when the border closed to those cattle, the plants weren't able to source enough cattle to operate at capacity. Some processors have laid off workers; some reduced hours of operation; and others have closed altogether.
Source: http://www.usagnet.com/story−national.cfm?Id=633&yr=2005

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

15. *June 22, Associated Press* — **Number of 2005 polio cases jumps.** The number of confirmed polio cases has reached 243 in Yemen, a country that was once believed to have been free of

the disease, the chief of the World Health Organization (WHO) said. Yemen accounts for nearly half of the 533 cases in the world this year as of June 15, said Lee Jong−wook, the WHO's director−general. A recent outbreak in Indonesia has brought the number of cases there to 51, he said. "The threat of a polio importation is a real and continuing one," Lee said. "The recent importation to Yemen and Indonesia remind us that we must continue to protect the children everywhere until the polio is stopped in the endemic countries."
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/22/AR2005062200338.html

16. *June 22, Genetic Engineering News* — **Testing of synthetic DNA vaccine against smallpox.** CytoGenix, Inc. announced that it has entered into an agreement with the University of Pennsylvania for animal studies using the company's proprietary synDNA technology to test a DNA vaccine against smallpox. David B. Weiner, Associate Professor, University of Pennsylvania Medical School, will conduct these proof−of−concept studies to determine the immunological activity of the synthetic DNA vaccine compared to a plasmid DNA vaccine. Weiner comments, "For the past fifteen years, we have worked to bring DNA vaccines into the public health mainstream. One of the chief impediments has been the high cost of pure clinical grade DNA. We are eager to conduct these experiments to determine if vaccines made by this method are as effective or more effective than current DNA vaccines." CytoGenix, Inc. is a Houston, TX, based biopharmaceutical company.
Source: http://www.genengnews.com/news/bnitem.aspx?name=554909XSL_NEWSML_TO_NEWSML_WEB.xml

17. *June 21, Government Computer News* — **Physician qualifications Web portal.** The Department of Health and Human Services (HHS) is seeking industry information about developing a nationwide verification system to provide the department with the professional qualifications of healthcare professionals responding to a disaster or public health emergency. HHS plans to develop a portal to provide access to the public and private data repositories that contain the qualifications of government medical incident officials, the department said in a request for information posted Monday, June 20 on FedBizOpps.gov. The portal would enable HHS to quickly authenticate professional qualifications −− including health−care providers' state license information, board certifications, any disciplinary actions and hospital privileges −− from a variety of sources during an emergency. The information would also be used for nonemergency situations for contingency planning.
Source: http://www.gcn.com/vol1_no1/daily−updates/36160−1.html

18. *June 20, Burnham Institute* — **Anthrax inhibitors identified.** A collaborative team of scientists, led by the Burnham Institute's Maurizio Pellecchia, has identified inhibitors of the anthrax toxin, termed lethal factor ("LF"), that could be developed into an emergency treatment for exposure to inhalation anthrax. Pulmonary anthrax, in which spores of the anthrax bacteria are inhaled, is typically fatal unless diagnosis is made at an early stage of infection, when antibiotics can provide a complete cure. At late stages in the disease, antibiotics can kill the anthrax bacteria, but do not affect LF secreted by the bacteria, which is sufficiently concentrated in the bloodstream. LF enters cells and inactivates a human protein called "mitogen−activated protein kinase" (MAPKK), disrupting the normal signaling pathways of the cell and inducing cell−death. Using a fragment−based approach based on assays conducted with highly sensitive nuclear magnetic resonance (NMR) techniques developed in Pellecchia's

laboratory, the scientists were able to identify a scaffold that served as a template for designing a preferred structure for small−molecule inhibitors of LF. Lead compounds were synthesized and validated as highly potent and selective against LF in vitro. Three lead compounds where tested in mice infected with anthrax spores, in combination with the antibiotic Ciprofloxacin. The survival rate for mice treated with each of the compounds tested in the combination therapy was two−fold over mice treated with Ciprofloxacin alone.
Source: http://www.burnham.org/NewsAndInformation/News/06−20−2005.as p

[Return to top]

Government Sector

19. *June 22, Associated Press* — **Security at Connecticut Capitol eases.** Security at the state Capitol will be loosened for the first time since the September 11 attacks, after budget problems led to the layoff of security guards who had been supplementing the building's regular police force. Since early 2002, the unarmed guards had monitored two unlocked entrances and two other checkpoints in the Legislative Office Building at yearly cost of nearly $400,000. The layoffs are part of the effort to keep the state budget under the spending cap, said House Speaker James A. Amann. Officials said the building's security would not be compromised, citing the Capitol's 24−member police force and an extensive system of video surveillance. "Cameras are on us 24−7 around that building," Amann said. "We are being watched."
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−capitol−security,0,1043428.story?coll=sns−ap−nation−headlines

[Return to top]

Emergency Services Sector

20. *June 21, New York Times* — **A team of rescuers rehearses for the worst in West Virginia.** A plaintive cry pierced the dusty darkness Tuesday, June 21, as a team of police officers and firefighters from New York City searched through mangled cars and trucks in a two−lane highway tunnel that appeared to have been hit by a bomb. This scene could have taken place in any big American city. But it played out in a training center near Standard, WV, where an expert team of search−and−rescue specialists tested their ability to respond to a weapon of mass destruction. The team, overseen by the city's Office of Emergency Management, is available to help with search−and−rescue efforts throughout the East. In August, the team will be at the top of a list of 28 national task forces to roll out on six hours' notice to any sort of major disaster, from a terrorist attack to a severe hurricane. The tunnel is used to train National Guard units and the emergency−services teams they sometimes assist, said Col. James A. Hoyer, the deputy commander for installations and homeland defense and the center's overseer. The federal government has spent $24 million on the facility, the Center for National Response, which has trained about 23,000 people, he said. Colonel Hoyer said his crew could create a variety of challenging locales and circumstances, from mountain caves like those used by al Qaeda in Afghanistan to a subway disaster, complete with an old trolley from Boston's Green Line.
Center for National Response: http://www.centerfornationalresponse.com/
Source: http://www.nytimes.com/2005/06/22/nyregion/22drill.html

21. *June 20, U.S. Air Force* — **Air Force holds accident response exercise in New Hampshire.** An accident response exercise called Granite Thunder 2005 took place recently at New Boston Air Force Station in New Hampshire. The exercise evaluated base and local emergency authorities' responses to a terrorist event, said Maj. Greg Tobin, 50th Space Wing deputy inspector general and exercise evaluator. The town of New Boston provides the bulk of emergency services for the base, one of eight satellite tracking stations the Air Force operates worldwide. For the exercise, base authorities parked a van on the side of the road and tipped it over alongside a training dummy used by local police and fire departments. The explosion and resulting scene created the illusion that a suicide bomber had attempted to gain entry to the base and, having been injured by the gate guard, crashed his vehicle and ended his life. Besides the exercise explosion, authorities dealt with the van's two other passengers who had escaped into the woods after wounding security forces Airmen. "This exercise helped a wide variety of New Hampshire emergency responders gain proficiency dealing with each other and New Boston," Major Tobin said.
Source: http://www.af.mil/news/story.asp?storyID=123010822

22. *June 17, Delaware Health and Social Services* — **Delaware's emergency response tested.** Delaware Health and Social Services' Division of Public Health (DPH) is conducting a large−scale disaster exercise called "Operation Diamond Shield II " this week at locations throughout the state. The simulation will demonstrate the state's ability to rapidly direct and treat large numbers of sick Delawareans. The exercise will test how well DPH's Preparedness Section works with public and private responders to a health emergency. Evaluators will study how the state's hospitals accept, assess and treat large numbers of volunteer patients, and how Acute Care Centers are established under emergency conditions. Acute Care Centers are created outside of hospital settings so the sick and injured can report there instead of hospital emergency rooms. Evaluators will assess the responsiveness and efficiency of emergency responders, epidemiologists and laboratory workers. Several agencies are expected to participate in "Operation Diamond Shield II," including the Centers for Disease Control and Prevention, Delaware hospitals and the Division of Public Health.
Source: http://www.dhss.delaware.gov/dhss/pressreleases/2005/disaste rdrill−061705.html

[Return to top]

Information Technology and Telecommunications Sector

23. *June 22, Government Technology* — **Arizona deploys new converged Internet Protocol communications network.** On Tuesday, June 21, the initial installation of over 5,000 Internet Protocol (IP) phones in nine Arizona State agencies was completed as part of an ongoing overhaul of the State's communications infrastructure. Arizona is aggressively transforming its network infrastructure to efficiently utilize taxpayers' money and improve service quality. At the heart of this transition is an initiative to replace the State's aging telephone network with a converged IP−based network that carries voice and data, and eventually video. "An IP telephone provides increased functionality over a traditional PBX (private branch exchange) based telephone, while eliminating the costs associated with maintaining a separate voice network. For state agencies and employees as well as taxpayers served by State communications systems, this new, converged network means will allow us to enable a range of

new applications such as unified messaging, which provides a single in−box for e−mail, voice mail and even fax," stated the State CIO and Director of the Arizona Government Information Technology Agency (GITA) Chris Cummiskey. Arizona has taken a leadership role in implementing this efficiency−driven initiative, which is presently under consideration among other states nationwide.
Source: http://www.govtech.net/news/news.php?id=94373

24. *June 21, Information Week* — **Malicious software not likely to have large impact on mobile devices until 2007.** Mobile phone and PDA users have more than two years to get ready for a quick−spreading worm, John Pescatore and John Girard, analysts at Gartner research. Client−side anti−virus software meant for cell phones and PDAs "certainly work", but vendors aren't selling them said Pescatore. In part that's because the threat of a fast−spreading malicious worm or virus has been overblown by security vendors. In fact, the conditions for a real threat−one that has the ability to infect more than 30 percent of mobile devices used in the enterprise−simply don't exist. The three factors that must exist before a Slammer− or MSBlast−style attack hits mobile devices, said Pescatore, are the large−scale adoption of smart phones, ubiquitous uses of wireless messaging to exchange executable files, and the convergence of operating systems to the point where one enjoys a majority share of the market. According to Pescatore and Girard, those three conditions won't co−exist until around the end of 2007. Furthermore, they believe that end−point security solutions for smart phones, cell phones, and PDAs are a waste of time because they often fail to block the most damaging viruses.
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=164901703

25. *June 21, SecurityFocus* — **Opera Web Browser dialog box origin spoofing vulnerability.** Opera Web Browser is prone to a dialog box origin spoofing vulnerability. An attacker may exploit this vulnerability to spoof an interface of a trusted Website. This issue may allow a remote attacker to carry out phishing style attacks. There is no solution at this time.
Source: http://www.securityfocus.com/bid/14009/info

26. *June 21, SecurityFocus* — **SpamAssassin malformed email header remote denial of service vulnerability.** SpamAssassin is prone to a remote denial of service vulnerability. This issue is due to a failure of the application to properly handle overly long email headers. An attacker may cause SpamAssassin to take inordinate amounts of time to check a specially crafted email message. By sending many malicious messages, it may be possible for attackers to cause extremely large delays in email delivery, denying service to legitimate users. See Source link for solution.
Source: http://www.securityfocus.com/bid/13978/solution

27. *June 21, SecurityFocus* — **Vipul Razor−agents multiple unspecified denial of service vulnerability.** Vipul Razor−agents is prone to multiple unspecified denial of service vulnerabilities. The first denial of service vulnerability exists in the discovery logic of Razor agents. The second issue exists in the preprocessing code of Razor agents. Both issues may be exploited to cause a denial of service for the vulnerable application. See Source link for solution.
Source: http://www.securityfocus.com/bid/13984/solution

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures. **US−CERT Operations Center Synopsis:** Activity on one of the ports associated with Windows' Server Message Block (SMB) protocol is climbing. A surge in activity targeting TCP port 445, which is associated with SMB related communications on Windows machines has been observed. This may indicate an increase in known attacks, such as password brute forcing, or the exploitation of known vulnerabilities, or may indicate activity related to the recent Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 1026 (−−−), 6881 (bittorrent), 27015 (halflife), 139 (netbios−ssn), 53 (domain), 137 (netbios−ns), 18152 (−−−), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

28. *June 22, New York Times* — **Three−year federal study urges safer skyscraper rules.** After an exhaustive, three−year study of the collapse of the World Trade Center, a federal panel will call for major changes in the planning, construction and operation of skyscrapers to help people survive not only terrorist attacks but also accidental or natural calamities, according to officials and draft documents. The recommendations include a call for a fundamental change in evacuation strategies for tall buildings: that everyone should have a way out in an emergency, replacing the current standard of providing evacuation capacity for a few floors near a fire or emergency. The panel also called for sturdier elevators and stairways, and found that current standards for testing fireproofing of steel for tall buildings are flawed. Taken together, the recommendations, by the National Institute of Standards and Technology, are likely to open an intense national debate over the costs of such changes and whether lessons for other skyscrapers can reasonably be drawn from the extraordinary events of September 11. The agency's proposals are not binding, but are meant to influence the policies of cities and states across the country. While the agency has revised certain aspects of its findings on what precisely happened at the trade center, the package of recommendations makes it clear that the agency has essentially held firm on its emphatic and demanding safety agenda for the next generation of tall buildings in America.
Source: http://www.nytimes.com/2005/06/22/nyregion/22towers.html?hp&ex=1119499200&en=8b9adea555ebc924&ei=5094&partner=homepage

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer